Cyclotomic Rings, Lattices and Space-Time Block Codes

Xiang-Gen Xia

Department of Electrical and Computer Engineering

University of Delaware, Newark, DE, USA

Email: {xxia}@ee.udel.edu

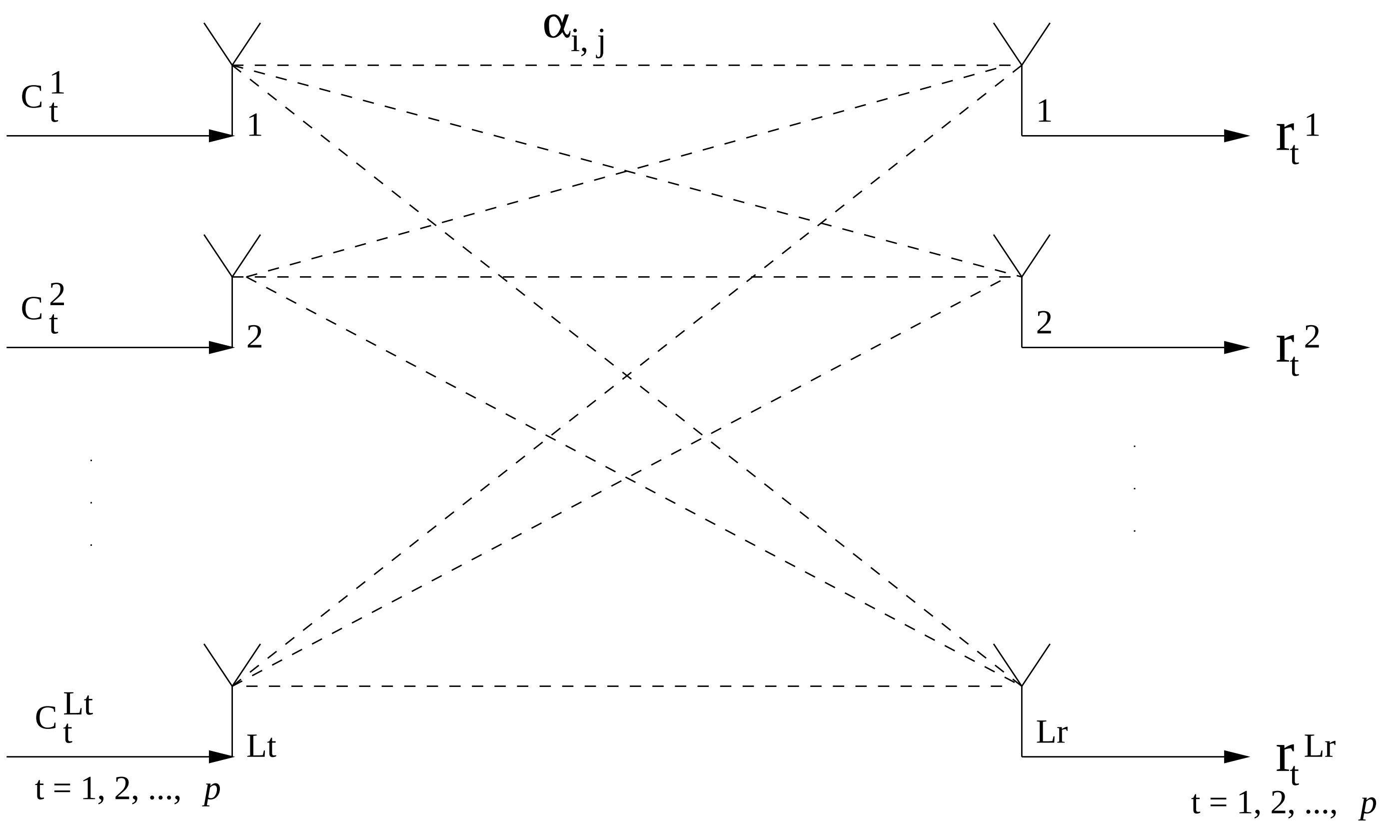
Sponsored by AFOSR

AFOSR Program Review, University of Delaware, June 2-4, 2004

OUTLINE

- Motivation
- Cyclotomic Rings
- Cyclotomic Lattices
  - Complex Lattices and Some Existing Examples
  - Cyclotomic Lattices of Full Diversity
  - Cyclotomic Diagonal Space-Time Codes
- Optimal Cyclotomic Lattices and Diagonal Space-Time Codes
- Some Simulation Results
- Conclusion and Future Research

Multiple Antenna System



L_t transmit antennas; L_r receive antennas; p is the time block size.

α_{ij} is the channel coefficient from ith transmit to jth receive antenna and is a random variable.

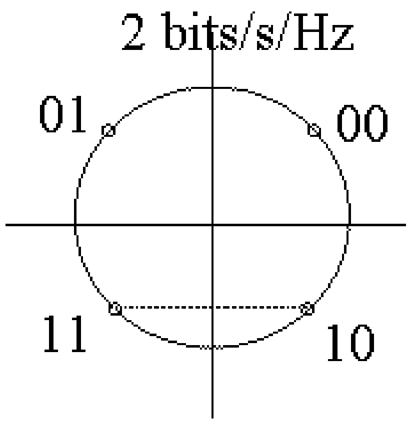
Advantage of Multi-Antenna System: Capacity Gain

- Teletar (1995), Foschini and Gans (1998) proved that the capacity of a multi-antenna system is proportional to $\min\{L_t, L_r\}$.
  - Theoretically, the more transmit and receive antennas, the better the capacity!
  - Practically, how can we achieve the capacity (gain)?
  - Shannon communication theory tells us that the capacity can be achieved by coding and modulation, **BUT HOW??**

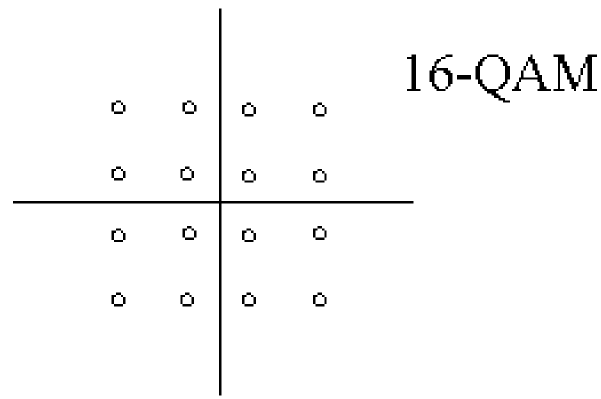
    —- **One of the most active research areas in communications theory!**

Single Antenna Coding and Modulation

- Low rate transmission: 1 bit modulated to 1 number/symbol (BPSK)
- High rate trasnmission: multiple bits modulated to 1 number/symbol (M-QAM, M-PSK)
- Consider 4, 14-QAM: 2, 4 bits become a complex number/symbol:



These 4 points are optimal:
The minimum distance is maximal



These 16 points are almost optimal

What is Multiple Antenna Coding and Modulation: Signal Model

- Transmit and receive signal model:

$$Y = AC + W,$$

where

$Y = (r_t^i)_{L_r \times p}$: Received signal matrix

$A = (\alpha_{ij})_{L_r \times L_t}$: Channel coefficient matrix

$C = (c_t^j)_{L_t \times p}$: Transmit signal matrix

$W = (w_{i,t})_{L_r \times p}$: Additive white Gassian noice (AWGN) matrix.

What is Multiple Antenna Coding and Modulation

- Multiple antenna coding/modulation: Binary information bits are modulated/mapped into $L_t \times p$ matrices and these matrices are taken from a pre-designed matrix set called *space-time code*.
- How to design a space-time code: It should be designed in such a way that the error probability at the receiver is minimized.

Space-Time Code Design Criteria

Based on the pair-wise error probability from the maximum-likelihood (ML) decoding, Guey-Fitz-Bell-Kuo and Tarokh-Seshadri-Calderbank proposed the following rank and diversity product criteria:

- **Rank criterion**: Any differece matrix of any two distinct matrices in a space-time code $\mathcal{C}$ has full rank;
- **Diversity product criterion** (or coding advantage or product distance):

$$\xi(\mathcal{C}) = \min_{C \neq \tilde{C} \in \mathcal{C}} |\det((C - \tilde{C})^{\dagger}(C - \tilde{C}))|$$

  is as large as possible.

Some Existing Space-Time Coding Schemes

- Space-time block codes
  - BLAST–No full diversity
  - Alamouti scheme-Orthogonal space-time block codes from orthogonal designs, quasi orthogonal space-time codes– Fast decoding with good performance BUT symbol rates are limited!
  - Unitary space-time codes: Group codes, Caley transforms, parametric codes, packing theory etc. – Good performance but no fast decoding in general, no systematic designs!
  - Space-time codes from binary linear codes – Performance is limited!
  - **Linear lattice based codes** – Fast sphere decoding, high rates, systematic: **My focus**
- Space-time trellis codes

Linear Lattice Based Space-Time Codes and Motivation

- BLAST schemes
- (Quasi) Orthogonal space-time codes (Alamouti, Tarokh et al, Jafarkhani, Tirkkonen et al etc.)
- Linear dispersive codes (Hassibi-Hochwald, Heath et al, Sandhu et al, etc.)
- Signal Space Diversity Codes and Diagonal Space-Time Codes using Algebraic Number Theory (Boutros-Viterbo, Giraud-Boutillon-Belfiore, Damen-Meraim-Belfiore, Sethuraman-Rajan, ...
  - The existing lattice based space-time block codes
    - ∗ Not **concrete** but simply some abstract algebraic numbers
    - ∗ Mostly based on square QAM, i.e., square lattice.
    - ∗ Not optimized in terms of diversity product

– The **focus** of this presentation:

  * Propose a general systematic and **concrete** cyclotomic full diversity lattices.
  * Propose optimal cyclotomic lattices and space-time block codes in terms of maximized diversity product for fixed mean signal power.

General Problem Description

- Let L_t be the number of transmit antennas.
- Let G be an $L_t \times L_t$ matrix and

$$[\mathbf{y}_1, \cdots, \mathbf{y}_{L_t}]^T = G[\mathbf{x}_1, \cdots, \mathbf{x}_{L_t}]^T,$$

  where $\mathbf{x}_i$ are information symbols.

- A diagonal space-time code Ω consists of $L_t \times L_t$ matrices of the form diag$(\mathbf{y}_1, \cdots, \mathbf{y}_{L_t})$.

- We are interested in such a diagonal space-time code Ω that

  (i) it has the full rank property, i.e., any difference matrix of any two distinct matrices in Ω has full rank; and

  (ii) its following diversity product is as large as possible:

$$\xi = \min_{\text{diag}(\mathbf{y}_1,\cdots,\mathbf{y}_{L_t})\neq\text{diag}(\mathbf{e}_1,\cdots,\mathbf{e}_{L_t})\in\Omega} \prod_{i=1}^{L_t} |\mathbf{y}_i - \mathbf{e}_i|^2,$$

  where the transmission signal mean power of $\mathbf{y}_i$ is fixed, or **equivalently**, the transmission signal mean power is minimized, when the diversity product is fixed.

Cyclotomic Rings

- Let $\zeta_m = \exp(\mathbf{j}\frac{2\pi}{m})$ be the mth root of unity.
- Let $\mathbb{Z}[\zeta_m]$ denote the ring generated by $\mathbb{Z}$, all integers, and ζ_m. It is called a *cyclotomic ring*.
- When $m = 4$, $\mathbb{Z}[\zeta_m] = \mathbb{Z}[\mathbf{j}]$ that is called Gaussian integers.
- When $m = 3, 6$, $\mathbb{Z}[\zeta_3] = \mathbb{Z}[\zeta_6]$ that is called Eisenstein integers.
- An important result from algebraic number theory: For a fixed L,

$$\min_{(0,\cdots,0)\neq(\mathbf{x}_1,\cdots,\mathbf{x}_L)\in(\mathbb{Z}[\zeta_m])^L} \prod_{i=1}^{L} |\mathbf{x}_i| = 1$$

  where $m = 3, 4, 6$, i.e., for Gaussian or Eisenstein integers.
- We next want to define **cyclotomic lattices.**

Real Lattices

- An n-dimensional *real lattice* $\Lambda_n(K)$ is a subset in $\mathbb{R}^n$:

$$\Lambda_n(K) = \left\{ \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = K \begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix} \middle| \; z_i \in \mathbb{Z} \text{ for } 1 \leq i \leq n \right\},$$

  where $\mathbb{Z}$ is the ring of all integers and K is an $n \times n$ real matrix of full rank and called the generating matrix of the real lattice $\Lambda_n(K)$ and $\det(\Lambda_n(K)) \triangleq |\det{(K)}|$.

- Every point $[x_1, x_2]^T$ in a two dimensional real lattice $\Lambda_2(K)$ is treated equivalently as a complex number $\mathbf{x} = x_1 + jx_2$ in the complex plane $\mathbb{C}$.

- For $\zeta_m = \exp(j\frac{2\pi}{m})$, we use Λ_{ζ_m} to denote the two dimensional real lattice with the generating matrix

$$K_{\zeta_m} = \begin{bmatrix} 1 & \cos(\frac{2\pi}{m}) \\ 0 & \sin(\frac{2\pi}{m}) \end{bmatrix} = \begin{bmatrix} 1 & \mathrm{Re}(\zeta_m) \\ 0 & \mathrm{Im}(\zeta_m) \end{bmatrix}.$$

Thus, $\Lambda_{\zeta_m} = \Lambda_2(K_{\zeta_m})$.

- $\Lambda_{\zeta_m} \subset \mathbb{Z}[\zeta_m]$, $\Lambda_{\zeta_4} = \mathbb{Z}[\zeta_4] = \mathbb{Z}[j]$, and $\Lambda_{\zeta_3} = \Lambda_{\zeta_6} = \mathbb{Z}[\zeta_3] = \mathbb{Z}[\zeta_6]$

Complex Lattices

- **Definition**: An n-dimensional complex lattice $\Gamma_n(G)$ over a two dimensional real lattice $\Lambda_2(K)$ is a subset of $\mathbb{C}^n$:

$$\Gamma_n(G) = \left\{ \begin{bmatrix} \mathbf{y}_1 \\ \vdots \\ \mathbf{y}_n \end{bmatrix} = G \begin{bmatrix} \mathbf{x}_1 \\ \vdots \\ \mathbf{x}_n \end{bmatrix} \middle| \; \mathbf{x}_i \in \Lambda_2(K), \;\; \text{for } 1 \leq i \leq n \right\},$$

where G is an $n \times n$ complex matrix of full rank and called the generating matrix of the complex lattice $\Gamma_n(G)$. The above complex lattice is called a full diversity lattice if it satisfies

$$\prod_{i=1}^{n} |\mathbf{y}_i| > 0$$

for any non-zero vector $[\mathbf{x}_1, \cdots, \mathbf{x}_n]^T \neq [0, \cdots, 0]^T$ in $(\Lambda_2(K))^n$.

- **Examples**

  – Rotated Codes Based on QAM on the Square Lattice: G_2 and G_4, 2-point and 4-point DFT matrices based on $\mathbb{Z}[\zeta_4]$ (Boutros-Viterbo (98) and Giraud-Boutillon-Belfiore (97))

  – Good Codes for Fading Channels as well as Gaussian Channels: D_4, E_6, E_8, G_2, G_3, G_4 based on $\mathbb{Z}[\zeta_4]$ and $\mathbb{Z}[\zeta_3]$ (Boutros-Viterbo (98) and Giraud-Boutillon-Belfiore (97))

  – Diagonal Algebraic Space-Time Block Codes – DAST Block Codes based on $\mathbb{Z}[\zeta_4]$: M_n (Boutros-Viterbo (98) and Damen-Meraim-Belfiore (02))

Cyclotomic Lattices

- For two positive integers n and m, let $N = mn$ and

$$L_t = \frac{\phi(N)}{\phi(m)},$$

where $\phi(N)$ and $\phi(m)$ are the Euler numbers of N and m, respectively.

- Then, there are total L_t distinct integers n_i, $1 \leq i \leq L_t$, with $0 = n_1 < n_2 < \cdots < n_{L_t} \leq n-1$ such that $1 + n_i m$ and N are co-prime for any $1 \leq i \leq L_t$.

- With these L_t integers, we define

$$G_{m,n} \triangleq \begin{bmatrix} \zeta_N & \zeta_N^2 & \cdots & \zeta_N^{L_t} \\ \zeta_N^{1+n_2 m} & \zeta_N^{2(1+n_2 m)} & \cdots & \zeta_N^{L_t(1+n_2 m)} \\ \vdots & \vdots & \ddots & \vdots \\ \zeta_N^{1+n_{L_t} m} & \zeta_N^{2(1+n_{L_t} m)} & \cdots & \zeta_N^{L_t(1+n_{L_t} m)} \end{bmatrix}_{L_t \times L_t},$$

where $\zeta_N = \exp(j\frac{2\pi}{N})$.

- **Definition**: An L_t dimensional complex lattice $\Gamma_{L_t}(G_{m,n})$ over Λ_{ζ_m} is called a cyclotomic lattice, where $G_{m,n}$ is defined above and Λ_{ζ_m} is the two dimensional real lattice with the generating matrix K_{ζ_m}. Its minimum product $d_{\min}(\Gamma_{L_t}(G_{m,n}))$ is defined by

$$d_{min}(\Gamma_{L_t}(G_{m,n})) \stackrel{\Delta}{=} \min_{[0,\cdots,\cdots,0]^T \neq [\mathbf{y}_1,\cdots,\mathbf{y}_{L_t}]^T \in \Gamma_{L_t}(G_{m,n})} \left| \prod_{i=1}^{L_t} \mathbf{y}_i \right| .$$

- Some equivalent forms of $G_{m,n}$:

$$G_{m,n} \stackrel{\Delta}{=} \text{diag}(\zeta_N, \zeta_N^{1+n_2 m}, \cdots, \zeta_N^{1+n_{L_t} m})\hat{G}_{m,n},$$

where

$$\hat{G}_{m,n} \triangleq \begin{bmatrix} 1 & \zeta_N & \cdots & \zeta_N^{L_t-1} \\ 1 & \zeta_N^{1+n_2 m} & \cdots & \zeta_N^{(L_t-1)(1+n_2 m)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta_N^{1+n_{L_t} m} & \cdots & \zeta_N^{(L_t-1)(1+n_{L_t} m)} \end{bmatrix}_{L_t \times L_t} .$$

$$G_{m,n} = \begin{bmatrix} \zeta_n^{n_1} & \zeta_n^{2n_1} & \cdots & \zeta_n^{L_t n_1} \\ \zeta_n^{n_2} & \zeta_n^{2n_2} & \cdots & \zeta_n^{L_t n_2} \\ \vdots & \vdots & \ddots & \vdots \\ \zeta_n^{n_{L_t}} & \zeta_n^{2n_{L_t}} & \cdots & \zeta_n^{L_t n_{L_t}} \end{bmatrix}_{L_t \times L_t} \quad \text{diag}(\zeta_N, \zeta_N^2, \cdots, \zeta_N^{L_t}).$$

- A difference with the existing results on this topic is that the above proposed cyclotomic lattice generating matrix is **concrete** and systematic.

- **Theorem 1**: A cyclotomic lattice is a full diversity lattice.

Cyclotomic Diagonal Space-Time Codes

- **Definition**: A diagonal cyclotomic space-time code Ω for L_t transmit antennas is defined by $\Omega = \{\text{diag}(\mathbf{y}_1, \cdots, \mathbf{y}_{L_t})\}$ where $\mathbf{y}_i$ for $1 \leq i \leq L_t$ are defined as follows:

$$[\mathbf{y}_1, \cdots, \mathbf{y}_{L_t}]^T = G_{m,n}[\mathbf{x}_1, \cdots, \mathbf{x}_{L_t}]$$

  where $[\mathbf{x}_1, \cdots, \mathbf{x}_{L_t}]^T \in \mathcal{S} \subset (\mathbb{Z}[\zeta_m])^{L_t}$ and $\mathcal{S}$ is a signal constellation for information symbols.

- **Theorem 2**: A diagonal cyclotomic space-time code has full diversity.

- $G_2 = \hat{G}_{4,2}$ and $G_4 = \hat{G}_{4,4}$.

- **Question**: For a transmit antenna number L_t, there are infinitely many cyclotomic lattices $G_{m,n}$ from infinitely many pairs (m, n). For a fixed L_t, which cyclotomic lattice is **optimal** in the sense that, its mean transmission power is minimized when its diversity product is fixed?

Optimal Cyclotomic Lattices

- The mean transmission signal power of signal points on a lattice is reciprocal to the packing density.
- From the packing theory, the packing density is reciprocal to the absolute value of the determinant of the generating matrix.
- The absolute value of the determinant of the generating matrix of a cyclotomic is

$$|\det(G_{m,n})|^2 \cdot |\det(K_{\zeta_m})|^{L_t}.$$

- **Criterion**: Let $\Gamma_{L_t}(G_{m_1,n_1})$ and $\Gamma_{L_t}(G_{m_2,n_2})$ be two L_t dimensional cyclotomic lattices over $\Lambda_{\zeta_{m_1}}$ and $\Lambda_{\zeta_{m_2}}$, respectively. We say cyclotomic lattice $\Gamma_{L_t}(G_{m_1,n_1})$ is *better than* cyclotomic lattice $\Gamma_{L_t}(G_{m_2,n_2})$, written as $\Gamma_{L_t}(G_{m_1,n_1}) \leq \Gamma_{L_t}(G_{m_2,n_2})$, if

$$|\det(G_{m_1,n_1})| \cdot |\det(\Lambda_{\zeta_{m_1}})|^{L_t/2} \leq |\det(G_{m_2,n_2})| \cdot |\det(\Lambda_{\zeta_{m_2}})|^{L_t/2},$$

  when their minimum products are the same, i.e., $d_{\min}(\Gamma_{L_t}(G_{m_1,n_1})) = d_{\min}(\Gamma_{L_t}(G_{m_2,n_2}))$.

- Define the following normalized minimum product

$$\gamma_{m,n} = \frac{d_{\min}(\Lambda_{L_t}(G_{m,n}))}{|\det(\Gamma_{\zeta_m})|^{L_t/2}|\det(G_{m,n})|}$$

- **Theorem 3**: If the number of transmit antennas has the form

$$L_t = \frac{\phi(3n)}{\phi(3)} \text{ or } \frac{\phi(6n)}{\phi(6)}, \quad \text{for some integer } n,$$

then the optimal cyclotomic lattice can be achieved by an Eisenstein cyclotomic lattice, i.e., $m = 3$ or $m = 6$, and the minimum product (or diversity product) of the optimal cyclotomic lattice is 1.

- Examples of such L_t are

$$L_t = 3^{r_1} p_2^{r_2-1}(p_2 - 1) \cdots p_k^{r_k-1}(p_k - 1),$$

where $k \geq 1$, $p_2, \cdots, p_k$ are distinct primes and different from 3, and $r_1 \geq 0$, $r_2 \geq 1, \cdots, r_k \geq 1$ are integers, which covers 2,3,4,6,8,9,10,12,16,18,20,22,24,27,28,30,32,....

- **Corollary**: For the listed numbers, L_t, of transmit antennas, the parameters (m, n) of the optimal cyclotomic lattices $\Gamma_{L_t}(G_{m,n})$ over Λ_{ζ_m} with generating matrix $G_{m,n}$ are listed in the following table.

L_t	(m,n) in $G_{m,n}$	$\gamma_{m,n}$
2	$(3,4),(4,3),(6,2)$	$\frac{1}{\sqrt{3}}$
3	$(3,3),(3,6),(6,3)$	$\frac{1}{4.1878}$
4	$(3,5),(3,10),(6,5)$	$\frac{1}{8.3852}$
6	$(3,7),(3,14),(6,7)$	$\frac{1}{84.2037}$
8	$(3,20),(4,15),(6,10)$	$\frac{1}{1.125\times 10^{3}}$
9	$(3,9),(3,18),(6,9)$	$\frac{1}{1.0303\times 10^{4}}$
10	$(3,11),(3,22),(6,11)$	$\frac{1}{2.3655\times 10^{4}}$
12	$(3,15),(3,30),(6,15)$	$\frac{1}{4.2981\times 10^{5}}$
16	$(3,40),(4,30),(6,20)$	$\frac{1}{3.24\times 10^{8}}$
18	$(3,21),(3,42),(6,21)$	$\frac{1}{1.1752\times 10^{10}}$
20	$(3,25),(3,50),(6,25)$	$\frac{1}{4.0484\times 10^{11}}$
22	$(3,23),(3,46),(6,23)$	$\frac{1}{4.083\times 10^{13}}$
24	$(3,35),(3,70),(6,35)$	$\frac{1}{9.8192\times 10^{13}}$
27	$(3,27),(3,54),(6,27)$	$\frac{1}{3.0205\times 10^{18}}$
28	$(3,29),(3,58),(6,29)$	$\frac{1}{7.3757\times 10^{18}}$

Optimal Diagonal Cyclotomic Space-Time Code Designs

- Optimal diagonal cyclotomic space-time block codes can be designed by
  - selecting optimal cyclotomic lattices
  - selecting signal points on the optimal cyclotomic lattices with the minimum mean transmission power (i) the information symbols are independently selected (ii) the information symbols are jointly selected.
- Design Examples

Diversity Products of Diagonal Codes for Two and Four Transmit Antennas

Bit rate	Space-Time Codes, $L_t = 2$				
b/s/Hz	$\mathbf{M}_2$-$\mathbb{Z}[j]$-QAM	G_2-$\mathbb{Z}[j]$-QAM	G_2-$\mathbb{Z}[j]$-Joint	$G_{6,2}$-Λ_{ζ_6}-QAM	$G_{6,2}$-Λ_{ζ_6}-Joint
2	$\frac{1}{4.47}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
3	$\frac{1}{5.5231}$	$\frac{1}{5}$	$\frac{1}{4.6562}$	$\frac{1}{4.3125}$	$\frac{1}{4.125}$
4	$\frac{1}{11.2}$	$\frac{1}{10}$	$\frac{1}{9.5703}$	$\frac{1}{8.75}$	$\frac{1}{8.2266}$

Bit rate	Space-Time Codes, $L_t = 4$				
b/s/Hz	$\mathbf{M}_4$-$\mathbb{Z}[j]$-QAM	G_4-$\mathbb{Z}[j]$-QAM	G_4-$\mathbb{Z}[j]$-Joint	$G_{6,5}$-Λ_{ζ_6}-QAM	$G_{6,5}$-Λ_{ζ_6}-Joint
2	$\frac{1}{640}$	$\frac{1}{256}$	$\frac{1}{94.15}$	$\frac{1}{64}$	$\frac{1}{43.0664}$
3	$\frac{1}{1000}$	$\frac{1}{400}$	$\frac{1}{323.2265}$	$\frac{1}{297.5625}$	$\frac{1}{170.514}$
4	$\frac{1}{4000}$	$\frac{1}{1600}$	$\frac{1}{1305.9}$	$\frac{1}{1225}$	$\frac{1}{681.8418}$

Simulation Results

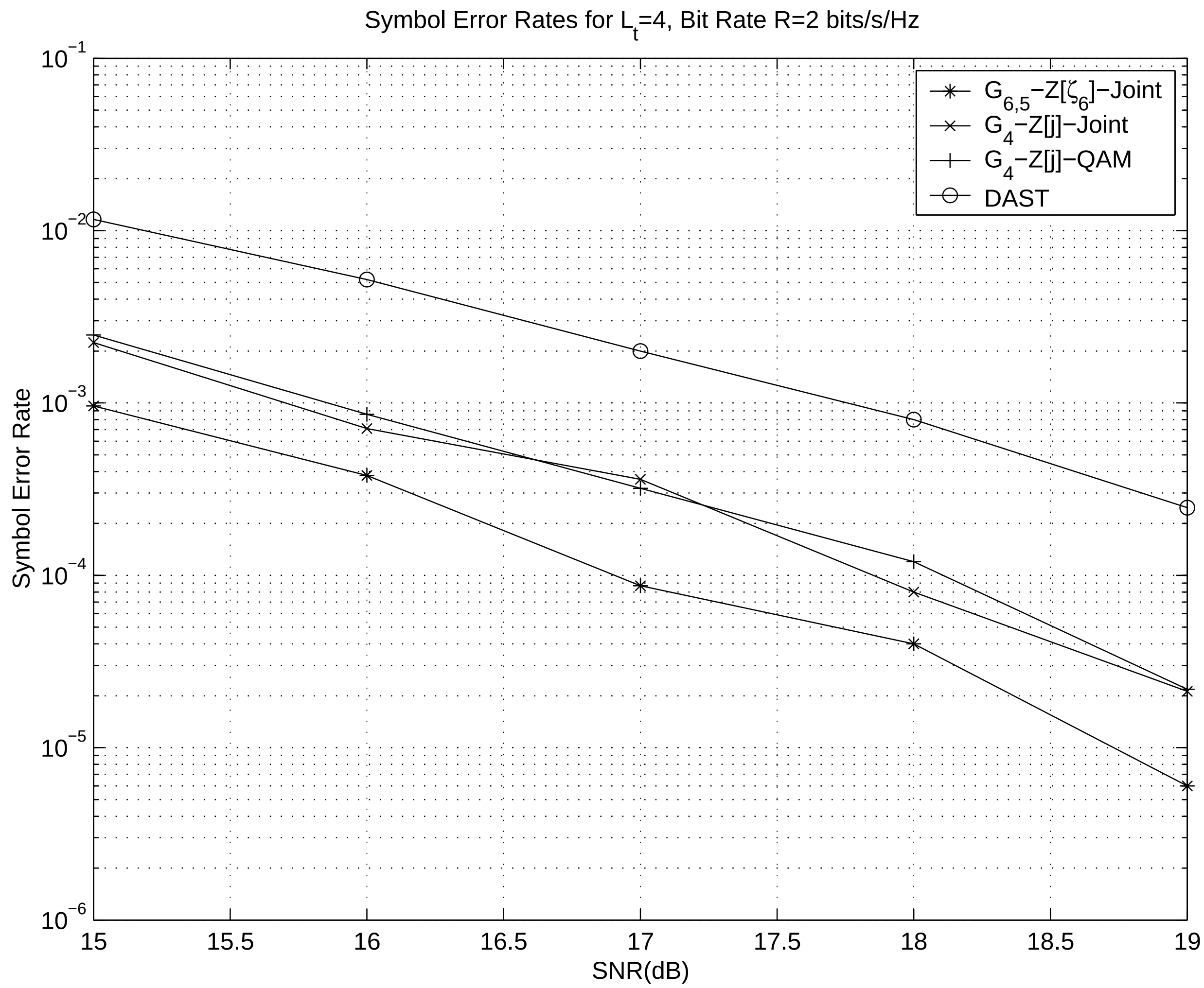


Figure 1: Symbol error rate, information rate $R = 2$ bits/s/Hz.

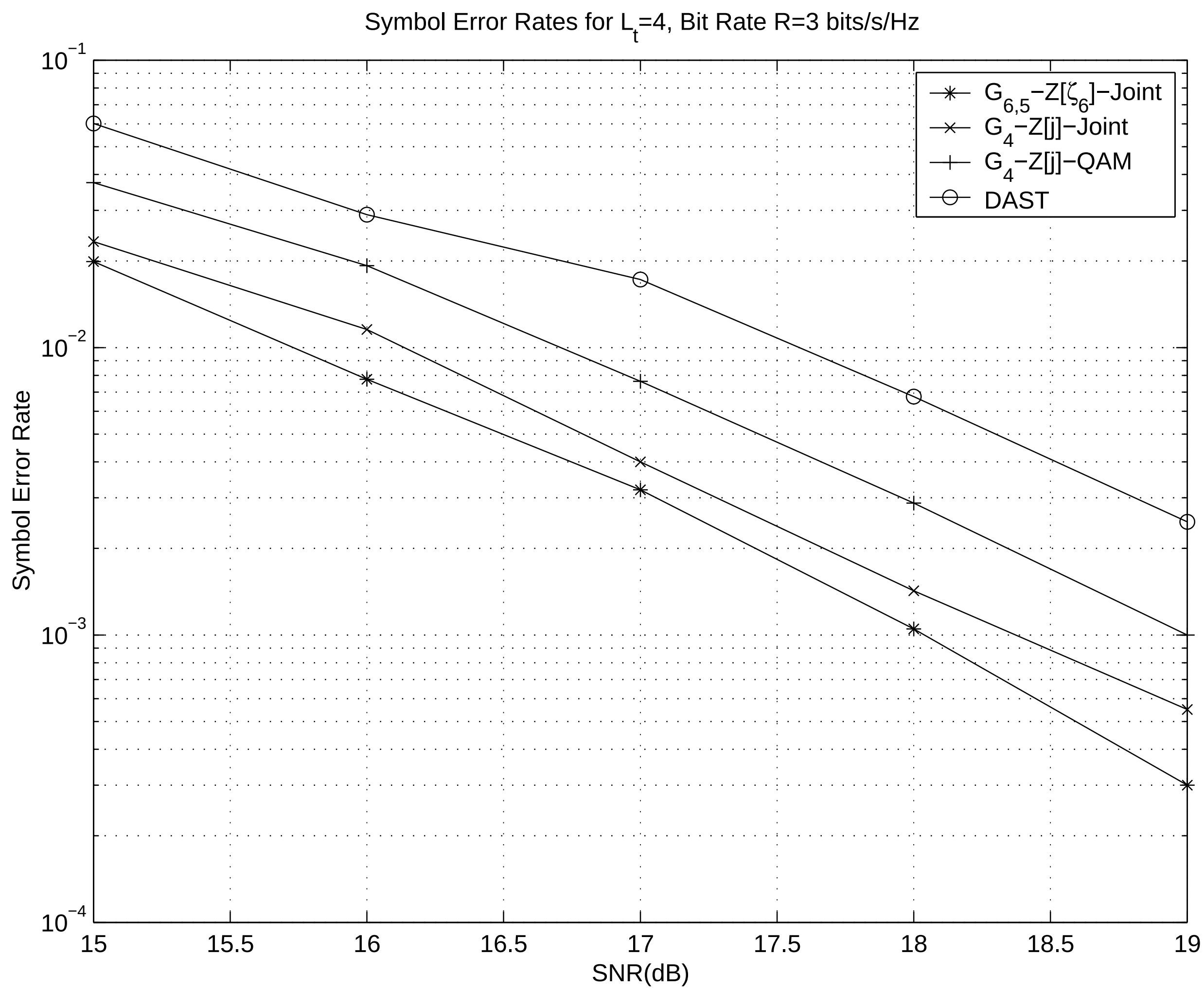


Figure 2: Symbol error rate, information rate $R = 3$ bits/s/Hz.

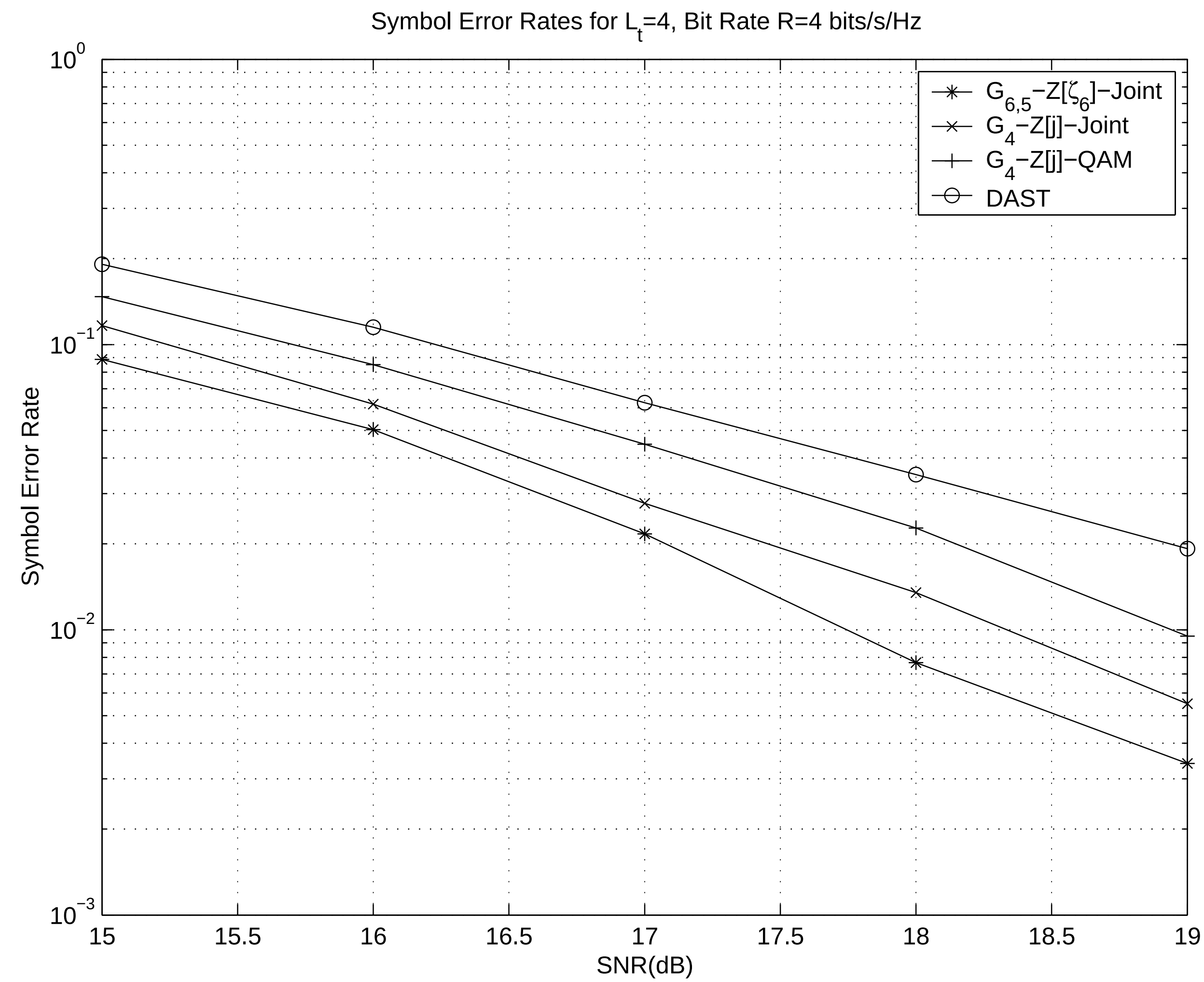
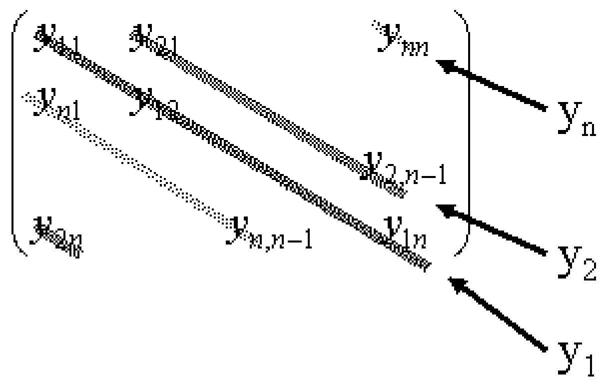


Figure 3: Symbol error rate, information rate $R = 4$ bits/s/Hz.

More Results

- We have generalized the optimal diagonal cyclotomic space-time codes to multi-layer cyclotomic space-time codes for 2 and 3 transmit antennas

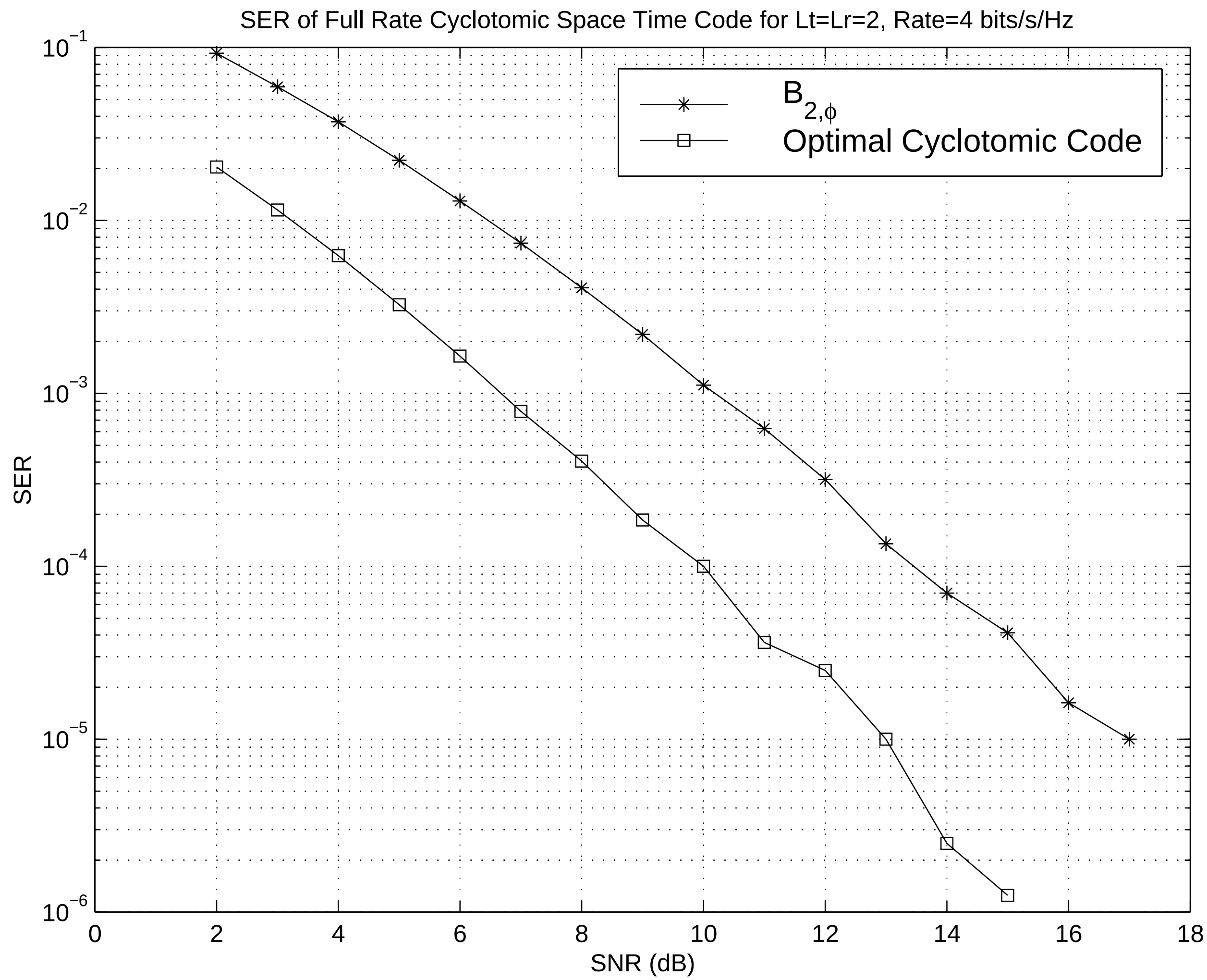


- Obtained some results on super-orthogonal trellis codes from QAM constellations

- Obtained some results on unitary space-time code designs from APSK signals

- Obtained a new family of recursive space-time trellis codes
- Obtained closed-form designs of complex orthogonal designs of rates $(k+1)/(2k)$ for $2k$ or $2k+1$ transmit antennas.
- Obtained some new unitary space-time codes with best and best known diversity product diversities by using packing theory.
- Obtained optimal quasi-orthogonal space-time codes with minimum decoding complexity.
- Obtained a fast iterative decoding algorithm for lattice based space-time codes based on soft interference cancellation.
- Applied some of our newly proposed space-time codes into a relay sensor network.

Simulation Result for Our Optimal Full Rate Full Diversity Code: $R = 4$ bits/s/Hz



Future Research

- Space-time code designs beyond cyclotomic rings: for example, $\mathbb{Z}[\zeta_m, \sqrt{5}]$
- Optimal multi-layer cyclotomic and quadratic space-time codes for more than 3 transmit antennas
- Space-time code designs for relay sensor networks to achieve optimal cooperative diversity
- Recursive space-time trellis code designs with optimal diversity products
- Super quasi orthogonal space-time trellis code designs

Conclusion

- Proposed systematic and concrete full diversity cyclotomic lattices and space-time block codes.
- Proposed optimal cyclotomic lattices and space-time block codes by minimizing the mean transmission power when their diversity products are fixed.

Acknowledgment

I would like to thank my following current and former group members:

Genyuan Wang, Weifeng Su, Xuebin Liang, Haiquan Wang, Huiyong Liao, Shengli Fu, Dong Wang, Yabo Li, Aijun Song